Stability of Grobner bases and ACGB (Computer Algebra : Design of Algorithms, Implementations and Applications)

AUTHOR(S):

Sato, Yosuke

CITATION:

Sato, Yosuke. Stability of Grobner bases and ACGB (Computer Algebra : Design of Algorithms, Implementations and Applications). 数理解析研究所講究録 2004, 1395: 24-30

ISSUE DATE:

2004-10

URL:

http://hdl.handle.net/2433/25922

数理解析研究所講究録 1395 巻 2004 年 24-30

Stability of Gröbner bases and ACGB

Yosuke Sato
Department of Mathematical Information Science,
Tokyo University of Science *

1 Introduction

Stability of Gröbner bases is an important notion in computer algebra. There have been published many papers by many authors. In [2] and [3], the following result is shown independently.

Theorem 1.1 (P.Gianni and M.Kalkbrener)
Let I be a zero-dimensional ideal of a polynomial ring $K[\bar{A}, X]$ over a field K where $\bar{A}$ denotes variables $A_1, \ldots, A_m$. Let $G = \{g_1(\bar{A}, X), \ldots, g_l(\bar{A}, X)\}$ be a Gröbner basis of I w.r.t. a term order $\geq$ of $T(\bar{A}, X)$ such that X is greater than any term in $T(\bar{A})$. Let $\bar{a}$ be an m-tuple of elements of the algebraic closure $\overline{K}$ of K which is a zero of the ideal $I \cap K[\bar{A}]$. Then, G becomes a Gröbner basis with the specialization by $\bar{a}$, that is $\{g_1(\bar{a}, X), \ldots, g_l(\bar{a}, X)\}$ becomes a Gröbner basis in $\overline{K}[X]$.
Here, $T(\bar{Y})$ denotes the set of all terms consisting of variables $\bar{Y}$.

For a polynomial ring $K[\bar{A}, \bar{X}]$ with several variables $\bar{X} = X_1, \ldots, X_n$, the above theorem is extended in [1] under some assumptions.

Theorem 1.2 (T.Becker)
Let I be an ideal of a polynomial ring $K[\bar{A}, \bar{X}]$ over a field K with variables $\bar{A}$ and $\bar{X}$ such that $I \cap K[\bar{A}]$ is a zero-dimensional radical ideal in $K[\bar{A}]$.
Let $G = \{g_1(\bar{A}, \bar{X}), \ldots, g_l(\bar{A}, \bar{X})\}$ be a Gröbner basis of I w.r.t. a term order $\geq$ of $T(\bar{A}, \bar{X})$ such that each variable X_i is greater than any term in $T(\bar{A})$ and the restriction of $\geq$ on $T(\bar{A})$ is a lexicographical term order. Let $\bar{a}$ be an m-tuple of elements of the algebraic closure $\overline{K}$ of K which is a zero of the ideal $I \cap K[\bar{A}]$. Then, G becomes a Gröbner basis with the specialization by $\bar{a}$, that is $\{g_1(\bar{a}, \bar{X}), \ldots, g_l(\bar{a}, \bar{X})\}$ becomes a Gröbner basis in $\overline{K}[\bar{X}]$ w.r.t. the term order that is a restriction of $\geq$ on $T(\bar{X})$.

In [4], the above result is further generalized to the following theorem.

Theorem 1.3 (M.Kalkbrener)
Let I be an ideal of a polynomial ring $K[\bar{A}, \bar{X}]$ over a field K with variables $\bar{A}$ and $\bar{X}$ such that $I \cap K[\bar{A}]$ is a zero-dimensional radical ideal in $K[\bar{A}]$. Let $G = \{g_1(\bar{A}, \bar{X}), \ldots, g_l(\bar{A}, \bar{X})\}$ be a D-Gröbner basis of I in the polynomial ring $(K[\bar{A}])[\bar{X}]$ over the coefficient ring $K[\bar{A}]$. Let $\bar{a}$ be an m-tuple of elements of the algebraic closure $\overline{K}$ of K which is a zero of the ideal $I \cap K[\bar{A}]$. Then, G becomes a Gröbner basis with the specialization by $\bar{a}$, that is $\{g_1(\bar{a}, \bar{X}), \ldots, g_l(\bar{a}, \bar{X})\}$ becomes a Gröbner basis in $\overline{K}[\bar{X}]$ w.r.t. the same term order.
(See Definition 4.1 for the definition of D-Gröbner bases.).

In both of the papers [1] and [4], they study when D-Gröbner bases are stable under specializations. The second paper also proves a more general fact from which we can see the assumption that $I \cap K[\bar{A}]$ is a zero-dimensional radical ideal is a boundary in some sense to keep the stability property. (See Theorem 3.3 of [4].) However either of them does not seem to give a simple insight why D-Gröbner bases are stable.

In [9, 10], we showed that alternative of comprehensive Gröbner bases can be defined in terms of Gröbner bases in polynomial rings over commutative Von Neumann regular rings, and we called them

*ysato@rs.kagu.tus.ac.jp

ACGB(Alternative Comprehensive Gröbner Bases). In [7], we further optimized ACGB to get the following result.

Theorem 1.4
Let $F = \{f_1(\bar{A}, \bar{X}), \ldots, f_s(\bar{A}, \bar{X})\}$ be a set of polynomials in $K[\bar{A}, \bar{X}]$, let I be a zero-dimensional proper radical ideal in $K[\bar{A}]$. Then the quotient ring $K[\bar{A}]/I$ becomes a commutative Von Neumann regular ring. Let $G = \{g_1(\bar{A}, \bar{X}), \ldots, g_l(\bar{A}, \bar{X})\}$ be a Gröbner basis of $\langle F \rangle$ in the polynomial ring $(K[\bar{A}]/I)[\bar{X}]$ over $K[\bar{A}]/I$. Then, $\{g_1(\bar{a}, \bar{X}), \ldots, g_l(\bar{a}, \bar{X})\}$ becomes a Gröbner basis of the ideal $\langle f_1(\bar{a}, \bar{X}), \ldots, f_s(\bar{a}, \bar{X}) \rangle$ for any m-tuple of elements $\bar{a}$ which lies on the variety $\mathbf{V}(I)$ in an algebraic extension field of K.

In this paper, we show that G in Theorem 1.3 actually becomes a Gröbner basis in the polynomial ring $(K[\bar{A}]/I \cap K[\bar{A}])[\bar{X}]$ over the commutative Von Neumann ring $K[\bar{A}]/I \cap K[\bar{A}]$. ¿From this result together with Theorem 1.4, Theorem 1.3 directly follows. Our proof is not only simple but also gives a natural and clear view why Gröbner bases are stable under specializations, since the notion of Gröbner bases in polynomial rings over commutative Von Neumann regular rings and the notion of comprehensive Gröbner bases are essentially same as is shown in [13].

We assume the reader is familiar with a theory of Gröbner bases in polynomial rings over commutative Von Neumann regular rings, which was introduced in [11]. Though we give a minimum review in section 2, we strongly recommend reading [6] or [11] for the reader who are not familiar with the theory. In section 2, we also prove some properties which will be used for proving our main result. In section 3, we give a brief review of ACGB. Though the contents is self contained, we also refer the reader to [7, 10] for more detailed description. Our main result is proved in section 4.

2 Von Neumann regular rings and Gröbner bases

A commutative ring R with identity 1 is called a *Von Neumann regular ring* if it has the following property: $\forall a \in R\ \exists b \in R \quad a^2 b = a$. For such a b, $a^* = ab$ and $a^{-1} = ab^2$ are uniquely determined and satisfy $aa^* = a$, $aa^{-1} = a^*$, and $(a^*)^2 = a^*$. Note that every direct product of fields is a Von Neumann regular ring. Conversely, any Von Neumann regular ring is shown to be isomorphic to a subring of a direct product of fields as follows.

Definition 2.1
Let R be a Von Neumann regular ring. If we define $\neg a = 1 - a$, $a \wedge b = ab$ and $a \vee b = \neg(\neg a \wedge \neg b)$ for each $a, b \in R$ such that $a^2 = a, b^2 = b$, then $(\{x \in R \mid x^2 = x\}, \neg, \wedge, \vee)$ becomes a boolean algebra, which is denoted by $B(R)$.

Considering $B(R)$ as a boolean ring, Stone representation theorem gives the following isomorphism Φ from $B(R)$ to a subring of $\prod_{I \in St(B(R))} B(R)/I$ by $\Phi(x) = \prod_{I \in St(B(R))} [x]_I$, where $St(B(R))$ is the set of all maximal ideals of $B(R)$. This representation of $B(R)$ is extended to a representation of R as follows.

Theorem 2.1 (Saracino-Weispfenning)
For a maximal ideal I of $B(R)$, if we put $I_R = \{xy \mid x \in R, y \in I\}$, then I_R is a maximal ideal of R. If we define a map Φ from R into $\prod_{I \in St(B(R))} R/I_R$ by $\Phi(x) = \prod_{I \in St(B(R))} [x]_{I_R}$, then Φ is a ring embedding.

A maximal ideal coincides with a prime ideal in a boolean ring. In the rest of the paper $St(B(R))$ is denoted by $Spec(B(R))$. We use p for an element of $Spec(B(R))$ as in the papers [11, 13]. We also use the same notations R_p to denote the field R/p_R and x_p to denote the element $[x]_{p_R}$ in R_p.

In the following unless mentioned, Greek letters α, β, γ are used for terms, Roman letters a, b, c for elements of R, and f, g, h for polynomials over R. Throughout this section, we work in a polynomial ring over R which is a Von Neumann regular ring unless mentioned. We also assume that some term order is given. The leading term of f is denoted by $lt(f)$ and its coefficient by $lc(f)$. By $li(f)$ we denote $lc(f)^*$. The leading monomial of f, i.e., $lc(f)lt(f)$ is denoted by $lm(f)$. The set of all terms consisting of variables $\bar{X}$ is denoted by $T(\bar{X})$.

Definition 2.2
For a polynomial $f = a\alpha + g$ with $lm(f) = a\alpha$, a monomial reduction $\rightarrow_f$ is defined by $ba\beta + h \rightarrow_f ba\beta + h - ba^{-1}\beta(a\alpha + g)$, where $ab \neq 0$ and $ba\beta$ need not be the leading monomial of $ba\beta + h$.

A monomial reduction $\rightarrow_F$ by a set F of polynomials is also naturally defined. When F is a finite set, $\rightarrow_F$ has a termination property. Using this monomial reduction, Gröbner bases are defined as follows.

Definition 2.3
Let I be an ideal of a polynomial ring over R. A finite subset G of I is called a Gröbner basis of I, if it satisfies the property that $f \in I$ if and only if $f \stackrel{*}{\rightarrow}_G 0$ for each polynomial f.
We simply say G is a Gröbner basis if G is a Gröbner basis of the ideal $\langle G \rangle$ generated by itself.

Note that a Gröbner basis G of I is clearly a basis of I. It is not difficult to show the following property.

Lemma 2.2
A finite subset G of an ideal I is a Gröbner basis of I if and only if $\langle \{lm(f)|f \in I\} \rangle = \langle \{lm(g)|g \in G\} \rangle$

Proof. Assume that G is a Gröbner basis of I. Let f be a non-zero polynomial in I. Since $f \stackrel{*}{\rightarrow}_G 0$, there must exist polynomials $g_1, \ldots, g_s \in G$ such that $lt(g_i)|lt(f)$ for each $i = 1, \ldots, s$ and $(li(g_1) \vee \cdots \vee li(g_s))li(f) = li(f)$. Define $c_1, \ldots, c_s \in R$ inductively as follows. $c_i = b_i li(g_i)$ for each $i = 1, \ldots, s$, where $b_i = 1 - (c_1 + \cdots + c_{i-1})$ for each $i = 2, \ldots, s$. (We put $b_1 = 1$ for convenience.) Then we have $c_i c_j = 0$ for each distinct i and j and $c_1 + \cdots + c_s = li(g_1) \vee \cdots \vee li(g_s)$. Since $lc(f) = li(f)lc(f)$, we have $lc(f) = (c_1 + \cdots + c_s)lc(f)$. Hence, $lm(f) = (c_1 + \cdots + c_s)lc(f)lt(f) = c_1 lc(f)lt(f) + \cdots + c_s lc(f)lt(f) = b_1 li(g_1)lc(f)lt(f) + \cdots + b_s li(g_s)lc(f)lt(f) = b_1 li(g_1)lc(f)lt(g_1)(lt(f)/lt(g_1)) + \cdots + b_s li(g_s)lc(f)lt(g_s)(lt(f)/lt(g_s)) = b_1 lc(g_1)^{-1} lc(g_1)lc(f)lt(g_1)(lt(f)/lt(g_1)) + \cdots + b_s lc(g_s)^{-1} lc(g_s)lc(f)lt(g_s)(lt(f)/lt(g_s)) = b_1 lc(g_1)^{-1} lc(f)(lt(f)/lt(g_1))lm(g_1) + \cdots + b_s lc(g_s)^{-1} lc(f)(lt(f)/lt(g_s))lm(g_s)$. It follows that $\langle \{lm(f)|f \in I\} \rangle \subseteq \langle \{lm(g)|g \in G\} \rangle$. $\langle \{lm(f)|f \in I\} \rangle \supseteq \langle \{lm(g)|g \in G\} \rangle$ is trivial.

Assume conversely that $\langle \{lm(f)|f \in I\} \rangle = \langle \{lm(g)|g \in G\} \rangle$.
To get a contradiction suppose there exists a non-zero polynomial f in I which is irreducible by $\rightarrow_G$. This means that $lc(f)lc(g) = 0$ for any g in G satisfying $lt(g)|lt(f)$. By our assumption, there exists $g_1, \ldots, g_s \in G$ and monomials $a_1\alpha_1, \ldots, a_s\alpha_s$ such that $lm(f) = a_1 lm(g_1)\alpha_1 + \cdots + a_s lm(g_s)\alpha_s$. Multiplying $lc(f)$ from both sides, we get a contradiction $lc(f)lm(f) = 0$. □

Definition 2.4
For a polynomial f, $li(f)f$ is called the boolean closure of f and denoted by $bc(f)$. A polynomial f such that $f = bc(f)$ is called boolean closed. Note that $bc(f)$ is boolean closed.

Lemma 2.3
Let G be a Gröbner basis of an ideal I, then $G' = \{bc(g)|g \in G\}$ also becomes a Gröbner basis of I.

Proof. By the definition of boolean closure, G' is clearly a subset of I. Since $lm(g) = lm(bc(g))$ for each polynomial g, $\langle \{lm(g)|g \in G\} \rangle = \langle \{lm(g)|g \in G'\} \rangle$. So, G' is a Gröbner basis of I by Lemma 2.1. □
The following result of [5] will be used for proving our main result.

Lemma 2.4
Let R be a commutative ring with identity, which need not to be a Von Neumann regular ring. Let I be an ideal in a polynomial ring $R[\bar{X}]$ and $G = \{g_1, \ldots, g_m\}$ be a finite subset of I. Then the following properties are equivalent:

- $\langle \{lm(f)|f \in I\} \rangle = \langle \{lm(g)|g \in G\} \rangle$
- *For any polynomial $f \in I$, f has a Gröbner representation w.r.t. G, that is there exist polynomials $p_1 \ldots, p_m$ such that $f = \sum_{i=1}^{m} p_i g_i$ and $lt(f) \geq lt(p_i)lt(g_i)$ for each $i = 1, \ldots, m$.*

We conclude this section with the following fact.

Lemma 2.5
For a polynomial f in a polynomial ring $R[\bar{X}]$ and $p \in Spec(B(R))$, f_p denotes the polynomial in $R_p[\bar{X}]$ given from f by replacing each coefficient a with a_p. For a set F of polynomials in $R[\bar{X}]$, F_p denotes the set $\{f_p|f \in F\} - \{0\}$. Let G be a Gröbner basis of an ideal I in a polynomial ring $R[\bar{X}]$.
Then G_p becomes a Gröbner basis of the ideal I_p in the polynomial ring $R_p[\bar{X}]$ for each $p \in Spec(B(R))$.

Proof. Note first that for each element e in R_p there exists an element a in R such that $a_p = e$. Hence, for each polynomial h in $R_p[\bar{X}]$ there exists a polynomial f in $R[\bar{X}]$ such that $f_p = h$, from which it follows that I_p is an ideal in $R_p[\bar{X}]$.
In case each element of G is boolean closed, this lemma is already shown in [11]. (Where the converse also holds.) If G is not a set of boolean closed polynomials, let $G' = \{bc(g)|g \in G\}$. Then G' is also a Gröbner basis of I by Lemma 2.2. Therefore, G'_p is also a Gröbner basis of I_p. We claim that G'_p is a subset of G_p. Let g be a polynomial in G. Note first the following two properties:

If $li(g)_p = 0$, then $bc(g)_p = 0$. If $li(g)_p = 1$, then $bc(g)_p = g_p$.

Since $li(g)_p$ is 0 or 1 for each p, we have $bc(g)_p = 0$ or $bc(g)_p = g_p$, from which our claim follows. Since G_p is clearly a subset of I_p, G_p is a Gröbner basis of I_p in $R_p[\bar{X}]$. □

3 ACGB

A polynomial ring $K[\bar{A}]$ over a field K with variables $\bar{A} = A_1, \ldots, A_m$ is not a Von Neumann regular ring. But considering a polynomial in $K[\bar{A}]$ as a function from K^m to K, $K[\bar{A}]$ can be considered as a subring of a Von Neumann regular ring K^{K^m}. This idea leads us to define an *ACGB*(Alternative Comprehensive Gröbner Basis) as follows.

Definition 3.1
Let F be a finite set of polynomials in a polynomial ring $K[\bar{A}, \bar{X}]$ over a field K with variables $\bar{A} = A_1, \ldots, A_m$ and $\bar{X} = X_1, \ldots, X_n$. Let G be a Gröbner basis of $\langle F \rangle$ in the polynomial ring $K^{K^m}[\bar{X}]$. G is called an ACGB of F with parameters $\bar{A}$.

Theorem 3.1
Let $G = \{g_1, \ldots, g_l\}$ be an ACGB of $F = \{f_1(\bar{A}, \bar{X}), \ldots, f_s(\bar{A}, \bar{X})\}$ with parameters $\bar{A}$. Then, for each m-tuple $\bar{a} = a_1, \ldots, a_m$ of elements in K, $G_{\bar{a}}$ becomes a Gröbner basis of the ideal $\langle \{f_1(\bar{a}, \bar{X}), \ldots, f_s(\bar{a}, \bar{X})\} \rangle$ in $K[\bar{X}]$. Where $G_{\bar{a}}$ denotes the set $\{g_{1\bar{a}}, \ldots, g_{l\bar{a}}\}$ of polynomials $g_{1\bar{a}}, \ldots, g_{l\bar{a}}$ in $K[\bar{X}]$ given from $g_1, \ldots, g_l$ by replacing each coefficient c with $c(\bar{a})$.
(Remember that c is an element of K^{K^m}).

Proof. Let $R = K^{K^m}$. Note that for any element c of R, $c^2 = c$ if and only if $c(\bar{a}) = 0$ or $c(\bar{a}) = 1$ for each element $\bar{a}$ of K^m. Hence, the boolean ring $B(R)$ consists of all c of R such that $c(\bar{a}) = 0$ or $c(\bar{a}) = 1$ for each element $\bar{a}$ of K^m. That is $B(R)$ is the direct product $\mathbf{Z}_2^{K^m}$ of the finite field $\mathbf{Z}_2$. (Note that $B(R)$ is not a subring of R.) Clearly the set $\{c \in B(R)|c(\bar{a}) = 0\}$ forms a prime ideal in $B(R)$ for any element $\bar{a}$ of K^m. Let $\bar{a}$ be an element of K^m and p be the prime ideal $\{c \in B(R)|c(\bar{a}) = 0\}$. Note also that the maximal ideal $p_R = \{xy|x \in R, y \in p\}$ in R has the following form: $p_R = \{c \in R|c(\bar{a}) = 0\}$. Remember that R_p is the quotient field R/p_R. Since $c - c' \in p_R$ if and only if $c(\bar{a}) = c'(\bar{a})$ for any c and c' in R, the mapping θ from R/p_R to K defined by $\theta([c]_{p_R}) = c(\bar{a})$ is an isomorphism. If we identify R/p_R with K by this isomorphism, $[c]_{p_R}$ is equal to $c(\bar{a})$. Remember that $[c]_{p_R}$ is denoted by c_p. So the theorem follows from Lemma 2.4. □

In ACGB, we implicitely assume that a specialization can take any value from K^m. If we give a restriction on specializations, we can generalize ACGB as follows.

Definition 3.2
Let I be an ideal in a polynomial ring $K[\bar{A}]$. Let $V \subseteq K^m$ be the variety of I in K^m, that is $V = \{\bar{a} \in K^m | f(\bar{a}) = 0$ for any $f \in I\}$. Let F be a finite set of polynomials in a polynomial ring $K[\bar{A}, \bar{X}]$. Let G be a Gröbner basis of $\langle F \rangle$ in thr polynomial ring $K^V[\bar{X}]$. G is called an ACGB-V of F with parameters $\bar{A}$ and a variety V.

We have the following theorem by an exactly same proof of Theorem 3.1.

Theorem 3.2
Let $V \subseteq K^m$ be the variety of an ideal in $K^m[\bar{A}]$. Let $G = \{g_1, \ldots, g_l\}$ be an ACGB-V of $F = \{f_1(\bar{A}, \bar{X}), \ldots, f_s(\bar{A}, \bar{X})\}$ with parameters $\bar{A}$ and a variety V. Then, for each m-tuple $\bar{a}$ in V, $G_{\bar{a}}$ becomes a Gröbner basis of the ideal $\langle F(\bar{a}) \rangle$ in $K[\bar{X}]$.

Let V be the variety of an ideal I. Let $K[V]$ denote a subring of K^V which consists of all elements that can be represented as polynomial functions. Note that $K[V]$ is isomorphic to the quotient ring $K[\bar{A}]/\mathbf{I}(V)$, where $\mathbf{I}(V)$ denotes the ideal $\{f \in K[\bar{A}] | f(\bar{a}) = 0 \text{ for every } \bar{a} \in V\}$. In general, $K[\bar{A}]/\mathbf{I}(V)$ is not a Von Neumann regular ring. However, in case $\mathbf{I}(V)$ is zero-dimensional, it becomes a Von Neumann regular ring. Since $\mathbf{I}(V)$ is a radical ideal, it can be represented as an intersection of distinct prime ideals $P_1 \cap \cdots \cap P_k$. If $\mathbf{I}(V)$ is zero-dimensional, each P_i is also zero-dimensional, so it is maximal. Therefore, $K[\bar{A}]/\mathbf{I}(V)$ is isomorphic to the direct product $K[\bar{A}]/P_1 \times \cdots \times K[\bar{A}]/P_k$ of fields by the Chinese remainder theorem. So, $K[\bar{A}]/\mathbf{I}(V)$ becomes a Von Neumann regular ring. These observations lead us to have the following theorem.

Theorem 3.3
Let $F = \{f_1(\bar{A}, \bar{X}), \ldots, f_s(\bar{A}, \bar{X})\}$ be a finite set of polynomials in a polynomial ring $K[\bar{A}, \bar{X}]$ with variables $\bar{A} = A_1, \ldots, A_m$ and $\bar{X} = X_1, \ldots, X_n$. Let I be a zero-dimensional proper radical ideal in $K[\bar{A}]$. Then the quotient ring $K[\bar{A}]/I$ becomes a Von Neumann regular ring. Let G be a Gröbner basis of $\langle F \rangle$ in the polynomial ring $(K[\bar{A}]/I)[\bar{X}]$ over $K[\bar{A}]/I$. Each coefficient of a polynomial $h(\bar{X})$ in $(K[\bar{A}]/I)[\bar{X}]$ is a member of $K[\bar{A}]/I$, so it can be represented by a polynomial in $K[\bar{A}]$. Hence, $h(\bar{X})$ can also be represented as a polynomial in $K[\bar{A}, \bar{X}]$. Therefore, G can be represented by a set of polynomials $\{g_1(\bar{A}, \bar{X}), \ldots, g_l(\bar{A}, \bar{X})\}$ in $K[\bar{A}, \bar{X}]$. Then, for any m-tuple $\bar{a}$ of elements in the algebraic closure $\overline{K}$ of K which is a zero of I, $\{g_1(\bar{a}, \bar{X}), \ldots, g_l(\bar{a}, \bar{X})\}$ becomes a Gröbner basis of the ideal $\langle f_1(\bar{a}, \bar{X}), \ldots, f_s(\bar{a}, \bar{X})\rangle$ in $\overline{K}[\bar{X}]$.

Proof. If K is an algebraically closed field, let V be the variety of I. Since $\mathbf{I}(V) = I$, $K[V]$ is isomorphic to $K[\bar{A}]/I$. Therefore G is actually a ACGB-V of F with parameters $\bar{A}$ and the variety V, from which the theorem directly follows from Theorem 3.2.
In case K is not an algebraically closed field, we need to optimize the above proof. Represent $I = P_1 \cap \cdots \cap P_k$ as an intersection of distinct prime(maximal) ideals in $K[\bar{A}]$. For each $i = 1, \ldots, k$, let $\bar{a}_i \in \overline{K}^m$ be a zero of P_i. If we put $K_i = \{f(\bar{a}_i) | f(\bar{A}) \in K[\bar{A}]\}$ for each i, K_i becomes a field which is isomorphic to $K[\bar{A}]/P_i$. Define a map Φ from $K[\bar{A}]/I$ to $K_1 \times \cdots \times K_k$ by $\Phi(f(\bar{A})) = (f(\bar{a}_1), \ldots, f(\bar{a}_k))$. Then Φ is an isomorphism. So, $B(K[\bar{A}]/I)$ can be considered as a boolean ring $\mathbf{Z}_2^{\{1,\ldots,k\}}$. Where, the set $\{c \in B(K[\bar{A}]/I) | c(\bar{i}) = 0\}$ forms a prime ideal in $B(K[\bar{A}]/I)$ for each $i = 1, \ldots, k$. (Actually any prime ideal has such a form since $B(K[\bar{A}]/I)$ is finite.) If we denote it by p_i, $(K[\bar{A}]/I)_{p_i}$ can be identified with K_i and $f(\bar{A})_{p_i}$ is equal to $f(\bar{a}_i)$ for each $f(\bar{A}) \in K[\bar{A}]/I$ by a similar reason as is described in the proof of Theorem 3.1. Hence, by Lemma 2.4, $\{g_1(\bar{a}_i, \bar{X}), \ldots, g_l(\bar{a}_i, \bar{X})\}$ becomes a Gröbner basis of the ideal $\langle f_1(\bar{a}_i, \bar{X}), \ldots, f_s(\bar{a}_i, \bar{X})\rangle$ in $K_i[\bar{X}]$. Since the Gröbner basis property is conservative under a field extension, it is also a Gröbner basis in $\overline{K}[\bar{X}]$. □

4 Stability of Gröbner bases

In this section we prove our main result.

Definition 4.1
Let I be an ideal of a polynomial ring $K[\bar{A}, \bar{X}]$ over a field K with variables $\bar{A}$ and $\bar{X}$. Let G be a finite subset of I. Consider $K[\bar{A}, \bar{X}]$ as a polynomial ring $(K[\bar{A}])[\bar{X}]$ over the coefficient ring $K[\bar{A}]$. If we have $\langle\{lm(f) | f \in I\}\rangle = \langle\{lm(g) | g \in G\}\rangle$ in $(K[\bar{A}])[\bar{X}]$ with a term order $\geq$ of $T(\bar{X})$, G is called a D-Gröbner basis of I in $(K[\bar{A}])[\bar{X}]$ w.r.t. $\geq$.

Theorem 4.1
Let I be an ideal of a polynomial ring $K[\bar{A}, \bar{X}]$ over a field K with variables $\bar{A}$ and $\bar{X}$ such that $I \cap K[\bar{A}]$ is a zero-dimensional proper radical ideal in $K[\bar{A}]$. Let $G = \{g_1(\bar{A}, \bar{X}), \ldots, g_l(\bar{A}, \bar{X})\}$ be a D-Gröbner basis of I in $(K[\bar{A}])[\bar{X}]$ w.r.t. a term order $\geq$ of $T(\bar{X})$. If we consider G as a set of polynomials in the polynomial ring $(K[\bar{A}]/I \cap K[\bar{A}])[\bar{X}]$ over the Von Neumann regular ring $K[\bar{A}]/I \cap K[\bar{A}]$, then G also becomes a Gröbner basis in this polynomial ring w.r.t. $\geq$.

Proof. Let R denote the Von Neumann regular ring $K[\bar{A}]/I \cap K[\bar{A}]$, and $\langle G\rangle_R$ denote the ideal generated by G in the polynomial ring $R[\bar{X}]$.

By Lemma 2.1 and Lemma 2.3, in order to see that G becomes a Gröbner basis of $\langle G\rangle_R$ in $R[\bar{X}]$, it suffices to show that each polynomial $h(\bar{X}) \in \langle G\rangle_R$ in $R[\bar{X}]$ has a Gröbner representation w.r.t. G in $R[\bar{X}]$. We can have a polynomial $h(\bar{A},\bar{X})$ in $K[\bar{A},\bar{X}]$ which represents $h(\bar{X})$ as is described in Theorem 3.3. We can also take $h(\bar{A},\bar{X})$ from I. We first claim that we can take $h(\bar{A},\bar{X})$ such as the leading coefficient of $h(\bar{A},\bar{X})$ in $(K[\bar{A}])[\bar{X}]$ is not in $I \cap K[\bar{A}]$. If this property does not hold, let $G_{\bar{A}}$ be a(any) Gröbner basis of $I \cap K[\bar{A}]$ in the polynomial ring $K[\bar{A}]$, replace $h(\bar{A},\bar{X})$ with the normal form of $h(\bar{A},\bar{X})$ by $G_{\bar{A}}$, then $h(\bar{A},\bar{X})$ has the desired property. Since G is a D-Gröbner basis of I in $(K[\bar{A}])[\bar{X}]$, we have its Gröbner representation $h(\bar{A},\bar{X}) = \sum_{i=1}^{l} p_i(\bar{A},\bar{X})g_i(\bar{A},\bar{X})$ in $(K[\bar{A}])[\bar{X}]$ by Lemma 2.3. Note also that $lt(h(\bar{A},\bar{X})$ is same in both of $(K[\bar{A}])[\bar{X}]$ and $R[\bar{X}]$. Hence, this Gröbner representation is also a Gröbner representation in $R[\bar{X}]$. □

Together with Theorem 3.3, we directly have the following.

Corollary 4.2
Let I be an ideal of a polynomial ring $K[\bar{A},\bar{X}]$ over a field K such that $I \cap K[\bar{A}]$ is a zero-dimensional radical ideal in $K[\bar{A}]$.
Let $G = \{g_1(\bar{A},\bar{X}),\ldots,g_l(\bar{A},\bar{X})\}$ be a D-Gröbner basis of I in $(K[\bar{A}])[\bar{X}]$ w.r.t. a term order $\geq$ of $T(\bar{X})$. Let $\bar{a}$ be an m-tuple of elements of the algebraic closure $\overline{K}$ of K which is a zero of the ideal $I \cap K[\bar{A}]$. Then, G becomes a Gröbner basis with the specialization by $\bar{a}$, that is $\{g_1(\bar{a},\bar{X}),\ldots,g_l(\bar{a},\bar{X})\}$ becomes a Gröbner basis in $\overline{K}[\bar{X}]$ w.r.t. $\geq$.

Proof. When $I \cap K[\bar{A}]$ is not a proper ideal, the result is trivial, otherwise apply Theorem 4.1 and Theorem 3.3. □

The following lemma describes a relationship between D-Gröbner bases and standard Gröbner bases.

Lemma 4.3
Let I be an ideal of a polynomial ring $K[\bar{A},\bar{X}]$ over a field K with variables $\bar{A}$ and $\bar{X}$. Let $G = \{g_1(\bar{A},\bar{X}),\ldots,g_l(\bar{A},\bar{X})\}$ be a Gröbner basis of I w.r.t. a term order $\geq$ such that each variable X_i is greater than any term in $T(\bar{A})$. Then G is a D-Gröbner basis of I in $(K[\bar{A}])[\bar{X}]$ w.r.t. the term order that is a restriction of $\geq$ on $T(\bar{X})$.

Proof. Since Lemma 2.1 and Lemma 2.3 also hold in any polynomial ring over a field, each polynomial f in I has a Gröbner representation w.r.t. G in $K[\bar{A},\bar{X}]$. By our assumption on the term order, it is also a Gröbner representation of f w.r.t. G in $(K[\bar{A}])[\bar{X}]$. □

By this lemma, the following facts are direct consequences from the above theorem and corollary.

Theorem 4.4
Let I be an ideal of a polynomial ring $K[\bar{A},\bar{X}]$ over a field K with variables $\bar{A}$ and $\bar{X}$ such that $I \cap K[\bar{A}]$ is a zero-dimensional proper radical ideal in $K[\bar{A}]$. Let $G = \{g_1(\bar{A},\bar{X}),\ldots,g_l(\bar{A},\bar{X})\}$ be a Gröbner basis of I w.r.t. a term order $\geq$ such that each variable X_i is greater than any term in $T(\bar{A})$. If we consider G as a set of polynomials in the polynomial ring $(K[\bar{A}]/I \cap K[\bar{A}])[\bar{X}]$ over the Von Neumann regular ring $K[\bar{A}]/I \cap K[\bar{A}]$, then G also becomes a Gröbner basis of the ideal $\langle G\rangle$ in this polynomial ring w.r.t. the term order that is a restriction of $\geq$ on $T(\bar{X})$.

Corollary 4.5
Let I be an ideal of a polynomial ring $K[\bar{A},\bar{X}]$ over a field K such that $I \cap K[\bar{A}]$ is a zero-dimensional radical ideal in $K[\bar{A}]$.
Let $G = \{g_1(\bar{A},\bar{X}),\ldots,g_l(\bar{A},\bar{X})\}$ be a Gröbner basis of I w.r.t. a term order $\geq$ such that each variable X_i is greater than any term in $T(\bar{A})$. Let $\bar{a}$ be an m-tuple of elements of the algebraic closure $\overline{K}$ of K which is a zero of the ideal $I \cap K[\bar{A}]$. Then, G becomes a Gröbner basis with the specialization by $\bar{a}$, that is $\{g_1(\bar{a},\bar{X}),\ldots,g_l(\bar{a},\bar{X})\}$ becomes a Gröbner basis in $\overline{K}[\bar{X}]$ w.r.t. the term order that is a restriction of $\geq$ on $T(\bar{X})$.

5 Remarks

The original definition of D-Gröbner bases is slightly different from ours. It is defined only in a plynomial ring $(K[A])[\bar{X}]$ with one variable A. Since the property of Lemma 2.1 is usually used for the definition

of Gröbner bases in polynomial rings over arbitrary commutative rings, our D-Gröbner bases are nothing but Gröbner bases in a plynomial ring $(K[\bar{A}])[\bar{X}]$ over the domain $K[\bar{A}]$.

The condition that $I \cap K[\bar{A}]$ is zero-dimensional is crucial for the results of section 4.

Example 5.1
$G = \{AX + Y^2 - 1, Y^3 - 1\}$ is a Gröbner basis w.r.t. the lexicographical term order $\geq$ such that $X > Y > A$. However, we get $\{Y^2 - 1, Y^3 - 1\}$ by specializing $A = 0$, which is not a Gröbner basis.

The condition that $I \cap K[\bar{A}]$ is a radical ideal is also crucial. The following is a counterexample given in [2].

Example 5.2
$G = \{X_1^2, X_1X_2, X_1X_3^2, AX_1 + X_2, X_2^2, X_2X_3 - X_3^2, AX_2, X_3^3, AX_3^2, A^2\}$ is a reduced Gröbner basis w.r.t. the lexicographical term order $\geq$ such that $X_1 > X_2 > X_3 > A$. However, we get $\{X_1^2, X_1X_2, X_1X_3^2, X_2, X_2^2, X_2X_3 - X_3^2, X_3^3\}$ by specializing $A = 0$, which is not a Gröbner basis.

Three theorems of section 3 are originally given for boolean closed Gröbner bases in [7, 9, 10]. In this paper, we optimize our proofs so that the theorems hold for arbitrary Gröbner bases.

References

[1] Becker,T. (1994). On Gröbner Bases under Specialization. Applicable Algebra in Engineering, Communication and Computing. 5, 1–8.

[2] Gianni,P. (1989). Properties of Gröbner bases under specializations. EUROCAL '87, J. H. Davenport Ed., Springer LNCS 378, 293–297.

[3] Kalkbrener,M. (1989). Solving systems of algebraic equations by using Gröbner bases. EUROCAL '87, J. H. Davenport Ed., Springer LNCS 378, 282–292.

[4] Kalkbrener,M. (1997). On the Stability of Gröbner Bases Under Specializations. J. Symb. Comp. 24/1, 51–58.

[5] Möller,H.M. (1988). On the Construction of Gröbner Bases Using Syzygies. J. Symb. Comp. 6/2-3, 345–359.

[6] Sato, Y. (1998). A new type of canonical Gröbner bases in polynomial rings over Von Neumann regular rings. International Symposium on Symbolic and Algebraic Computation (ISSAC 98), Proceedings, 317–321

[7] Sato, Y., Suzuki, A. and Nabeshima, K. (2003). ACGB on Varieties, Proceedings of the Sixth International Workshop on Computer Algebra in Scientific Computing(CASC 2003), 313–318.

[8] Saracino, D., Weispfenning, V. (1975). On algebraic curves over commutative regular rings, Model Theory and Algebra, a memorial tribute to A. Robinson, Springer LNM 498, 307–387.

[9] Suzuki, A. and Sato, Y. (2002). An Alternative approach to Comprehensive Gröbner Bases. International Symposium on Symbolic and Algebraic Computation (ISSAC 2002), Proceedings, 255–261.

[10] Suzuki, A. and Sato, Y.(2003). An Alternative approach to Comprehensive Gröbner Bases. J. Symb. Comp. 36/3-4 649–667.

[11] Weispfenning, V. (1989). Gröbner bases in polynomial ideals over commutative regular rings, EUROCAL '87, J. H. Davenport Ed., Springer LNCS 378, 336–347.

[12] Weispfenning, V. (1992). Comprehensive Gröbner bases, J. Symb. Comp. 14/1, 1–29.

[13] Weispfenning, V. (2003). Comprehensive Gröbner bases and regular rings, To appear in J. Symb. Comp.